10/711132

| Ref # | Hits | Search Query | DBs | Default Operator | Plurals | Time Stamp |
|---|---|---|---|---|---|---|
| L1 | 13 | "6820199".pn. or "10011496" or "10710127" or "10710972" "10248604" | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:15 |
| L2 | 672 | 713/170 | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:15 |
| L3 | 4549 | 713/170 or 713/176 or 713/175 or 713/156 or 380/282 or 380/285 or 705/57 or 705/64 | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:16 |
| L4 | 0 | "digital signatuure" and "public key" and "private key" and account$1 and authenticat$3 and compar$4 and database | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:18 |
| L5 | 1520 | "digital signature" and "public key" and "private key" and account$1 and authenticat$3 and compar$4 and database | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:18 |
| L6 | 268 | 5 and 3 | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:18 |
| L7 | 62 | 5 and 2 | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:18 |
| L8 | 83 | wheeler.inv. and ann | US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB | OR | OFF | 2005/11/20 20:18 |

PORTAL USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

"digital signature" and "public key" and "private key" and data

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used digital signature and public key and private key and database and authenticat$3

Found **1,674** of **166,953**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search

Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Fast and secure distributed read-only file system

Kevin Fu, M. Frans Kaashoek, David Mazières

February 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 1

**Publisher:** ACM Press

Full text available: pdf(317.54 KB) Additional Information: full citation, abstract, references, index terms

Internet users increasingly rely on publicly available data for everything from software installation to investment decisions. Unfortunately, the vast majority of public content on the Internet comes with no integrity or authenticity guarantees. This paper presents the self-certifying read-only file system, a content distribution system providing secure, scalable access to public, read-only data.The read-only file system makes the security of published content independent from that of the distri ...

**Keywords**: File systems, read-only, security

2 Cryptosystems: Securely combining public-key cryptosystems

Stuart Haber, Benny Pinkas

November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security**

**Publisher:** ACM Press

Full text available: pdf(416.51 KB) Additional Information: full citation, abstract, references, citings, index terms

It is a maxim of sound computer-security practice that a cryptographic key should have only a single use. For example, an RSA key pair should be used only for public-key encryption or only for digital signatures, and not for both.In this paper we show that in many cases, the simultaneous use of related keys for two cryptosystems, e.g. for a public-key encryption system and for a public-key signature system, does not compromise their security. We demonstrate this for a variety of public-key encry ...

3 Secret key distribution protocol using public key cryptography

Amit Parnerkar, Dennis Guster, Jayantha Herath

October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1

**Publisher:** Consortium for Computing Sciences in Colleges

Full text available: pdf(74.93 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography. The authentication process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication in which, both participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

4 An authorization model for a public key management service

Pierangela Samarati, Michael K. Reiter, Sushil Jajodia

November 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 4

**Publisher:** ACM Press

Full text available: pdf(337.73 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Public key management has received considerable attention from both the research and commercial communities as a useful primitive for secure electronic commerce and secure communication. While the mechanics of certifying and revoking public keys and escrowing and recovering private keys have been widely explored, less attention has been paid to access control frameworks for regulating access to stored keys by different parties. In this article we propose such a framework for a key management ser ...

**Keywords**: Access control, authorizations specification and enforcement, public key infrastructure

5 Role-based access control on the web

February 2001 **ACM Transactions on Information and System Security (TISSEC)**, Volume 4 Issue 1

**Publisher:** ACM Press

Full text available: pdf(331.03 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Current approaches to access control on the Web servers do not scale to enterprise-wide systems because they are mostly based on individual user identities. Hence we were motivated by the need to manage and enforce the strong and efficient RBAC access control technology in large-scale Web environments. To satisfy this requirement, we identify two different architectures for RBAC on the Web, called user-pull and server-pull. To demonstrate feasibility, we im ...

**Keywords**: WWW security, cookies, digital certificates, role-based access control

6 SPV: secure path vector routing for securing BGP

Yih-Chun Hu, Adrian Perrig, Marvin Sirbu

August 2004 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '04**, Volume 34 Issue 4

**Publisher:** ACM Press

Full text available: pdf(236.82 KB) Additional Information: full citation, abstract, references, index terms

As our economy and critical infrastructure increasingly relies on the Internet, the insecurity of the underlying border gateway routing protocol (BGP) stands out as the Achilles heel. Recent misconfigurations and attacks have demonstrated the brittleness of BGP. Securing BGP has become a priority.In this paper, we focus on a viable deployment path to secure BGP. We analyze security requirements, and consider tradeoffs of mechanisms that achieve the requirements. In particular, we study how to se ...

**Keywords**: BGP, Border Gateway Protocol, interdomain routing, routing, security

7 Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration
Constantinos F. Grecas, Sotirios I. Maniatis, Iakovos S. Venieris
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
**Publisher:** Kluwer Academic Publishers
Full text available: pdf(107.24 KB) Additional Information: full citation, abstract, references, index terms

The logic ruling the user and network authentication as well as the data ciphering in the GSM architecture is characterized, regarding the transferring of the parameters employed in these processes, by transactions between three nodes of the system, that is the MS, actually the SIM, the visited MSC/VLR, and the AuC, which is attached to the HLR in most cases. The GPRS and the UMTS architecture carry the heritage of the GSM's philosophy regarding the user/network authentication and the data ciphe ...

**Keywords**: PKIs, PLMNs, asymmetric cryptography

8 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure
Albert Levi, M. Ufuk Caglayan, Cetin K. Koc
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
**Publisher:** ACM Press
Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

**Keywords**: Digital certificates, key management, nested certificates, public key infrastructure

9 Separating key management from file system security
David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel
December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5
**Publisher:** ACM Press
Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

10 Encryption and Secure Computer Networks
Gerald J. Popek, Charles S. Kline

December 1979 **ACM Computing Surveys (CSUR)**, Volume 11 Issue 4
**Publisher:** ACM Press
Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings, index terms

11 Efficient verifiable encryption (and fair exchange) of digital signatures
Giuseppe Ateniese
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security**
**Publisher:** ACM Press
Full text available: pdf(781.40 KB) Additional Information: full citation, abstract, references, citings, index terms

A fair exchange protocol allows two users to exchange items so that either each user gets the other's item or neither user does. In [2], verifiable encryption is introduced as a primitive that can be used to build extremely efficient fair exchange protocols where the items exchanged represent digital signatures. Such protocols may be used to digitally sign contracts.This paper presents new simple schemes for verifiable encryption of digital signatures. We make us ...

**Keywords**: contract signing problem, digital signatures, fair exchange, proof of knowledge, public-key cryptography, verifiable encryption

12 A secure and private system for subscription-based remote services
Pino Persiano, Ivan Visconti
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
**Publisher:** ACM Press
Full text available: pdf(241.65 KB) Additional Information: full citation, abstract, references, index terms

In this paper we study privacy issues regarding the use of the SSL/TLS protocol and X.509 certificates. Our main attention is placed on subscription-based remote services (e.g., subscription to newspapers and databases) where the service manager charges a flat fee for a period of time independent of the actual number of times the service is requested.We start by pointing out that restricting the access to such services by using X.509 certificates and the SSL/TLS protocol, while preserving the in ...

**Keywords**: Access control, anonymity, cryptographic algorithms and protocols, privacy, world-wide web

13 Verifiable encryption of digital signatures and applications
Giuseppe Ateniese
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
**Publisher:** ACM Press
Full text available: pdf(258.12 KB) Additional Information: full citation, abstract, references, index terms

This paper presents a new simple schemes for verifiable encryption of digital signatures. We make use of a trusted third party (TTP) but in an *optimistic* sense, that is, the TTP takes part in the protocol only if one user cheats or simply crashes. Our schemes can be used as primitives to build efficient fair exchange and certified e-mail protocols.

**Keywords**: Certified e-mail, contract signing, digital signatures, fair exchange, proof of knowledge, public-key cryptography

14 Digital signatures with RSA and other public-key cryptosystems
Dorothy E. Denning
April 1984 **Communications of the ACM**, Volume 27 Issue 4
**Publisher:** ACM Press
Full text available: pdf(374.39 KB) Additional Information: full citation, references, citings, index terms

**Keywords**: cryptanalysis, cryptographic, hashing, homomorphism, protocol

15 Authentication in distributed systems: theory and practice
Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
November 1992 **ACM Transactions on Computer Systems (TOCS)**, Volume 10 Issue 4
**Publisher:** ACM Press
Full text available: pdf(3.37 MB) Additional Information: full citation, abstract, references, citings, index terms, review

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegated authority. The theory shows how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We ...

**Keywords**: certification authority, delegation, group, interprocess communication, key distribution, loading programs, path name, principal, role, secure channel, speaks for, trusted computing base

16 Network security via private-key certificates
Don Davis, Ralph Swick
September 1990 **ACM SIGOPS Operating Systems Review**, Volume 24 Issue 4
**Publisher:** ACM Press
Full text available: pdf(256.46 KB) Additional Information: full citation, abstract, citings, index terms

We present some practical security protocols that use private-key encryption in the public-key style. Our system combines a new notion of *private-key certificates*, a simple key-translation protocol, and key-distribution. These certificates can be administered and used much as public-key certificates are, so that users can communicate securely while sharing neither an encryption key nor a network connection.

17 Trustworthy Web sites: An abuse-free fair contract signing protocol based on the RSA signature
Guilin Wang
May 2005 **Proceedings of the 14th international conference on World Wide Web**
**Publisher:** ACM Press
Full text available: pdf(196.63 KB) Additional Information: full citation, abstract, references, index terms

A fair contract signing protocol allows two potentially mistrusted parities to exchange their commitments (i.e., digital signatures) to an agreed contract over the Internet in a fair way, so that either each of them obtains the other's signature, or neither party does. Based on the RSA signature scheme, a new digital contract signing protocol is proposed in this paper. Like the existing RSA-based solutions for the same problem, our protocol is not only fair, but also optimistic, since the third ...

**Keywords**: RSA, contract signing, cryptographic protocols, digital signatures, e-commerce, fair-exchange, security

18 Security and Authentication with Digital Signatures
Robb Shecter
August 1997 **Linux Journal**
**Publisher:** Specialized Systems Consultants, Inc.
Full text available: html(13.22 KB) Additional Information: full citation, references, index terms

19 Securing the global, remote, mobile user
Walt Curtis, Lori Sinton
March 1999 **International Journal of Network Management**, Volume 9 Issue 1
**Publisher:** John Wiley & Sons, Inc.
Full text available: pdf(982.14 KB) Additional Information: full citation, abstract, index terms

Electronic commerce is inevitable and will reshape our lives, but before true electronic commerce environments can be realized, it will be necessary to secure your enterprise against outside attacks on its electronic information and provide controls for authorized access to that information. Copyright © 1999 John Wiley & Sons, Ltd.

20 Authentication in distributed systems: theory and practice
Butler Lampson, Martín Abadi, Michael Burrows, Edward Wobber
September 1991 **ACM SIGOPS Operating Systems Review , Proceedings of the thirteenth ACM symposium on Operating systems principles SOSP '91**, Volume 25 Issue 5
**Publisher:** ACM Press
Full text available: pdf(2.33 MB) Additional Information: full citation, abstract, references, citings, index terms

We describe a theory of authentication and a system that implements it. Our theory is based on the notion of principal and a "speaks for" relation between principals. A simple principal either has a name or is a communication channel; a compound principal can express an adopted role or delegation of authority. The theory explains how to reason about a principal's authority by deducing the other principals that it can speak for; authenticating a channel is one important application. We use the th ...

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next